Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

Before U.S. House Committee on Ways and Means
Subcommittee on Social Security

April 14, 2011

Electronic Employment Verification

Chairman Johnson, Ranking Member Becerra and members of the Subcommittee

On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates across the country, we write to express our concerns regarding E-Verify and to oppose any legislative proposal that would expand its use or require a national ID card with a biometric component. E-Verify has proven to be a flawed and burdensome electronic employment eligibility screening system that imposes unacceptable burdens on America's workers, businesses and society at large. A biometric ID system would be unworkable and impose significant privacy and civil liberties costs. The costs to lawful workers, businesses, and taxpayers associated with both these proposals are significant while the benefits are speculative.

Electronic Employment Verification

The ACLU opposes a mandatory Electronic Employment Verification System (EEVS) for five reasons:

(i) it poses unacceptable threats to American workers' privacy rights by increasing the risk of data surveillance and identity theft;

(ii) data errors in Social Security Administration ("SSA") and Department of Homeland Security ("DHS") files will wrongly delay or block the start of employment for lawful American workers and may lead to discrimination;

(iii) it lacks sufficient due process procedures to protect workers injured by such data errors;

(iv) neither SSA or DHS are able to implement such a system and SSA's ability to continue to fulfill its primary obligations to the nation's retirees and disabled individuals would deteriorate; and

(v) it will lead to rampant employer misuse in both accidental and calculated ways.

I. Mandating Electronic Employment Eligibility Verification Poses Unacceptable Threats to American Workers' Privacy Rights

A nationwide mandatory EEVS would be one of the largest and most widely accessible databases ever created in the U.S. Its size and openness would be an irresistible target for identity theft. Additionally, because the system would cover everyone (and be stored in a searchable format), it could lead to even greater surveillance of Americans by the intelligence community, law enforcement and private parties.

The current E-Verify system, implemented in a small fraction of the country's workplaces, contains an enormous amount of personal information including names, photos (in

some cases), social security numbers, phone numbers, email addresses, workers' employer and industry, and immigration information like country of birth. It contains links to other databases such as the Customs and Border Patrol (CBP) TECS database (a vast repository of Americans' travel history) and the Bureau of Citizenship and Immigration Services (CIS) BSS database (all immigration fingerprint information from US VISIT and other sources).[1]

The data in E-Verify, especially if combined with other databases, would be a gold mine for intelligence agencies, law enforcement, licensing boards, and anyone who wanted to spy on American workers. Because of its scope, it could form the backbone for surveillance profiles of every American. It could be easily combined with other data such as travel, financial, or communication information. 'Undesirable' behaviors – from unpopular speech to gun ownership to paying for items with cash – could be tracked and investigated by the government. Some of these databases linked to E-Verify are already mined for data. For example, the TECS database uses the Automated Targeting System (ATS) to search for suspicious travel patterns. Such data mining would be even further enhanced by the inclusion of E-Verify information

Without proper restrictions, American workers would be signing up for never-ending digital surveillance involuntarily every time they applied for a job. In order to help protect Americans' privacy, we recommend that Congress limit the retention period for queries to the E-Verify system to three to six months, unless it is retained as part of an ongoing compliance investigation or as part of an effort to cure a non-confirmation. This is a reasonable retention limitation for information necessary to verify employment. By comparison, information in the National Directory of New Hires, which is used on an ongoing basis to allow states to enforce child support obligations, is deleted after either 12 or 24 months.[2] The current retention period for E-Verify (set by regulation) is an astonishing 10 years. Deadbeat dads have greater privacy protections than American workers.

We also recommend strict limits on the use of information in any employment verification system. It should only be used to verify employment or to monitor for employment-related fraud. There should be no other federal, state, or private purpose. However, as a recent Westat report commissioned by CIS points out, any employer who signs on to a memorandum of understanding (MOU) can access E-Verify and therefore the data in the system could be used for other purposes. For example, such data could provide information about whether a mortgage or credit applicant is likely to be a poor credit risk.[3] Data should be bound by strict privacy rules, such as those that protect census data, which sharply limit both the disclosure and use of that information.[4]

Additionally, the system must guard against data breaches and attacks by identity thieves. Since the first data breach notification law went into effect in California at the beginning of 2004, more than 510 million records have been hacked, lost or disclosed improperly.[5] In 2007, it

[1] 73 Fed. Reg. 75449.
[2] The data retention limitation for the National Directory of New Hires is governed by 42 U.S.C. §653 (i).
[3] Westat Report, p 201
[4] Protections for census data can be found at 13 U.S.C. §9.
[5] Privacy Rights Clearinghouse Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

was reported that the FBI investigated a technology firm with a $1.7 billion DHS contract after it failed to detect "cyber break-ins".[6] The December 2010 GAO Report on E-Verify repeatedly references the risk of identity theft associated with the system. In one example, Immigration and Customs Enforcement (ICE) found that 1,340 employees of a meat processing plant were unauthorized workers even though each had been processed through E-Verify. Of the 1,340 unauthorized workers, 274 were charged with identity theft, including using valid Social Security numbers of others in order to work[7]. Data breaches continue to be a contributing factor to identity theft and a constant erosion of Americans' privacy and sense of security. An E-Verify database must not be subject to such threats.[8]

II. Data Errors Will Injure Lawful Workers by Delaying Start Dates or Denying Employment Altogether and May Lead to Discrimination

Recent government reports acknowledge that huge numbers of SSA and DHS files contain erroneous data that would cause "tentative non-confirmation"(TNC) of otherwise work-eligible employees and, in some cases, denial of their right to work altogether. CIS reported that 2.6%, or over 211,000 workers, received a TNC and, according to the Westate report, about 0.8% of these TNCs are erroneous.[9] Since only 0.3% of those mistaken TNCs were resolved, approximately 0.5%, or **80,000 legal workers,** were improperly denied the right to work due to faults in the system.[10] In many of these cases workers simply don't have the time or don't know they have the right to contest their determinations and seek different employment. Finding another job is a difficult option for many unemployed Americans in this economy and certainly means countless hours of red tape and frustration.

In American cities and states where E-Verify has been implemented, the results have been disastrous. A survey of 376 immigrant workers in Arizona (where use of E-Verify is required) found that 33.5% were fired immediately after receiving a TNC and never given chance to correct errors in the system. Furthermore, not one of those workers was notified by the employer, as required in the MOU, that he or she had the right to appeal the E-Verify finding. When Los Angeles County audited its use of E-Verify for 2008-09, it found that 87% of its E-Verify findings were erroneous. Implementing a system this flawed nationwide would be a train wreck for American workers.

These error rates are caused by a variety of factors. First, women or men who changed their names at marriage, divorce or re-marriage may have inconsistent files or may never have informed either SSA or DHS of name changes. Second, simple key stroke or misspelling errors contribute to the volume of erroneous data. Third, individuals with naming conventions that differ from those in the Western world may have had their names anglicized, transcribed improperly, or inverted. The GAO predicted that if E-Verify were made mandatory for new

---

[6] Ellen Nakashima and Brian Krebs, *Contractor Blamed in DHS Data Breaches*, WASHINGTON POST, Sept. 24, 2007.
[7] GAO, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain,* p. 24
[8] The breech last week at the Dallas based marketing firm Epsilon which revealed millions of Americans names and email addresses was only the most recent example of this trend.
[9] Westat Report, *Findings of the E-Verify Program Evaluation*, can be found at: http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf
[10] GAO, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain,* p.19.

hires nationwide, approximately 164,000 citizens per year would receive a TNC just for name change related issues. [11] It would be even more damaging if applied not just to new hires, but to existing workers as well.

The high number of error rates occurring among certain cultural groups can lead to an appearance of discrimination in the employment process. Five out of 25 employers acknowledged to GAO that TNCs were more likely to occur with Hispanic employees having hyphenated or multiple surnames.[12] Additionally the TNC rate for employees who were eventually authorized to work was approximately 20 times higher for foreign-born employees than for U.S.-born employees from April through June of 2008.[13] These striking disparities could easily lead employees to believe they were being judged on more than just their credentials. Moreover, employers may shy away from hiring non-native-born individuals or those with foreign names because of a fear they would be harder to clear through the system.

III. Pending Legislative Proposals Lack Meaningful Due Process Protections for Lawful Workers Injured by Data Errors

Workers injured by data errors will need a means of quickly and permanently resolving data errors so they do not become presumptively unemployable. Workers face two distinct challenges. The first is to learn that there are errors in their record and the second is the lack of fundamental due process protections in resolving those errors.

Self-Check

We commend the USCIS for beginning the process of creating a self-check system that allows workers to check on their E-Verify data. It is a fundamental privacy principle that individuals should have access to their own information in order to assure its completeness and correctness. However, it is important to note that this self-check process is still in its infancy and has only been rolled out on a limited basis.

We have some specific concerns about how the self-check program will be implemented. First of all, self-check is a tool for allowing workers to correct their records; it must not be used as a pre-screening tool. If employers were to impose a self-check requirement – effectively serving as an E-Verify pre-screening tool – they would shift the cost from the employer to the employee – and, in keeping with the statistics cited above, those costs would fall disproportionately on members of minority classes. This would undermine the anti-discrimination provisions built into the system to ensure that authorized workers are able to contest TNCs and document their eligibility to work.

Second, to the system must protect the privacy of both employers and employees. Considering high rates of identity fraud associated with the E-Verify system, it is no surprise that individuals are very concerned about the retention of their personal information in a database to

[11] *Id.* p. 19.
[12] *Id*. p. 20.
[13] *Id*. p. 40

which more and more people are gaining access. There must be clearly defined limits in regard to potential sharing of personal information.

Third, there must be an option for self-check access to people without credit histories. If self-check relies on background check information, then it will be unavailable to populations of foreign nationals who have only recently arrived in the U.S. and have not yet developed a credit history. This would include some of those with the most complicated immigration situations such as refugees, asylum seekers, and people with temporary protected status.[14]

Due Process Protections

Senior officials in the DHS Privacy Office have said that individuals face formidable challenges in correcting inaccurate or inconsistent information. The Office of Special Counsel for Immigration-Related Unfair Employment Practices and DHS Office of Civil Rights and Civil Liberties have both said that employees have expressed difficulty in understanding the TNC notification letters and the process by which they have to correct errors. Moreover, as of 2009 the average response time for these Privacy Act requests was a staggering 104 days.[15] This is time that an employee would be unable to work under a mandatory E-Verify system. Congress must prevent the creation of a new employment blacklist – a "No-Work List" – that will consist of would-be employees who are blocked from working because of data errors and government red tape.

Under current law there are no due process protections for those who lose their jobs due to government or employer errors. The best current model for due process protections can be found in Title II of the ''Comprehensive Immigration Reform for America's Security and Prosperity Act of 2009, H.R. 4321 from the 111th Congress. This provision would have created worker protections for both tentative and final non-confirmations, allowed workers to recover lost wages when a government error cost them a job, limited retention of personal information, and created accuracy requirements for the system.

IV. Government Agencies are Unprepared to Implement a Mandatory Employment Eligibility Prescreening System

As government reports evaluating E-Verify have repeatedly made clear, both SSA and DHS are woefully unprepared to implement a mandatory employment eligibility pre-screening system. The most recent GAO report expressed concerns over how CIS has estimated the cost of E-Verify. It found that the estimates do not reliably depict current E-Verify cost and resource needs for mandatory implementation and that they fail to fully assess the extent to which their workload costs could increase in the future.[16] In order to implement such a system, both agencies would need to hire hundreds of new, full-time employees and train staff at every SSA field office. DHS has an enormous backlog of unanswered Freedom of Information Act (FOIA) requests from lawful immigrants seeking their immigration files. Those files, many of which are

[14] The American Immigration Lawyers Association, *E-Verify Self Check Program*, November 29, 2010
[15] Department of Homeland Security, 2009 Annual Freedom of Information Act Report to the Attorney General of the United States
[16] Peck, Amy, *Latest Report on E-Verify: the Good, the Bad, and the Unresolved*, January 20, 2011

decades old, are the original source of numerous data errors. If DHS cannot respond to pending information requests in a timely fashion now, how much worse will the problem be when lawful immigrants, including naturalized citizens, lawful permanent residents, and visa holders need the documents immediately to start their next jobs? Consequently, DHS would need to hire hundreds more employees to respond to these FOIAs.

Businesses seeking to comply with any newly imposed system would also put additional strain on these government agencies. Problems can be anticipated in attempting to respond to employers' requests and in establishing connectivity for businesses located in remote regions or that do not have ready access to phones or the internet. These agency deficiencies will surely wreak havoc on independent contractors and the spot labor market for short-term employment.

Scaling up the existing software platform for E-Verify to respond to the enormous task of verifying the entire national workforce is likely to be a very difficult task. It makes little sense to adopt a system that is pre-destined to cause chaos within these agencies, not to mention the lives of the thousands of Americans wrongfully impacted.

V. CIS has Not Been Able to Achieve a Sufficient Degree of Employer Compliance in Order to Protect Worker's Rights

Despite the fact that CIS has more than doubled the number of staff tasked with monitoring employers' use of E-Verify since 2008, it still does not have the means to effectively identify and address employer misuse or abuse of the system. A recent report from the SSA Office of the Inspector General (OIG) found that SSA itself had failed to comply with many of regulations put in place to protect employees. They failed to confirm the employment of 19% of the 9,311 new employees hired for fiscal year 2008 through March 31, 2009 and, of those who were processed, they did not comply with the 3-day time requirement for verifying eligibility. The OIG also found that SSA verified the employment eligibility of 26 employees who were not new hires but had sought new positions within the agency, 31 volunteers who were not federal employees and 18 job applicants who SSA did not hire.[17] If the government is unable to maintain compliance within its own agencies, we cannot expect private businesses to follow the regulations put in place to protect workers.

Employer misuse has resulted in discrimination and anti-worker behavior in the past and there is no reason to suggest that pattern will change with a new verification system in place. From the inception of E-Verify, the Government Accountability Office and DHS studies have repeatedly documented various types of misuse. The CIS's Westat report also confirmed the fact that many employers were engaging in prohibited activity. Of the employers they contacted, they found that 17.1% admitted to restricting work assignments until authorization was confirmed; 15.4% reported delaying training until employment authorization was confirmed; and 2.4% reported reducing pay during the verification process.

If Congress imposes a mandatory system, it will need to create effective enforcement mechanisms that prevent the system from being a tool for discrimination in hiring. Such

[17] Social Security Administration, Office of the Inspector General, *The Social Security Administration's Implementation of the E-Verify Program for New Hires*, A-03-09-29154, January 6, 2010.

discriminatory actions will be difficult to prevent and even more difficult to correct. Congress should ask: how will the government educate employers and prevent misuse of E-Verify or any similar system?

Biometric National ID System

In response to concerns about the E-Verify system it has been suggested that a possible solution is the use of biometric identification.[18] The ACLU opposes the use of biometric identification because it effectively creates a national ID system with enormous negative implications for privacy, civil liberties and due process.

I. A Biometric National ID System Will Create a Hugely Expensive New Federal Bureaucracy and Will Not Stop Unauthorized Employment

In order to understand the practical problems with national ID, it is necessary understand how the system would work. The key to a biometric system is the verification of the individual. In other words, an individual must visit a government agency and must present documents such as a birth certificate or other photo ID that prove his or her identity. The agency must then fingerprint the person (or link to some other biometric) and place the print in a database. The agency might also place the biometric on an identification card. Such a process would create a quintessential national ID system because it would be nationwide, would identify everyone in the country, and would be necessary to obtain a benefit (in this case the right to work).

The closest current analogy to this system is a trip to the Department of Motor Vehicles to obtain a drivers' license. The federalizing of that system (without the addition of a new biometric) under the Real ID Act was estimated to cost more than $23 billion if carried out to completion, though 24 states have rejected the plan, putting its completion in grave doubt.[19] The cost to build such a system from scratch would be even more staggering. It would involve new government offices across the country, tens of thousands of new federal employees and the construction of huge new information technology systems. Every worker would have to wait in long lines, secure the documents necessary to prove identity, and deal with the inevitable government mistakes. Imagine the red tape necessary to provide documentation for 150 million U.S. workers. It is far beyond the capacity of any existing federal agency.

These problems are not hypothetical. After spending billions, the United Kingdom effectively abandoned its efforts to create a biometric national ID card, making it voluntary. Dogged by public opposition, data privacy concerns, and extensive technical problems, the program has been an embarrassment for the British government.

II. A Biometric National ID System Will Not Prevent Unauthorized Employment

Despite a popular assumption to the contrary, a biometric national ID system would largely fail to solve the problem of undocumented immigration. Security systems must be

[18] A biometric is a physical characteristic of an individual that can be used to uniquely identify them. Common examples include fingerprints, DNA and facial characteristics.
[19] 72 Fed. Reg. 10820.

judged not by their successes, but rather by their failures. After enduring a host of bureaucratic hassles and costs, most Americans would likely be able to enroll in the biometric system. But that does not make the system a success – those workers were already working lawfully. The system only succeeds if it keeps the undocumented workers in this country from securing employment and a biometric national ID system is unlikely to do that.

The first and most obvious failure is that this system would do nothing about employers who opt out of the system altogether (work "off the books"). Already, by some reports, more than 12 million undocumented immigrants are working in the United States. Many of these workers are part of the black market, cash wage economy. Unscrupulous employers who rely on below-market labor costs will continue to flout the imposition of a mandatory employment eligibility pre-screening system and biometric national ID. These unscrupulous employers will game the system by running only a small percentage of employees through the system or by ignoring the system altogether. In the absence of enforcement by agencies that lack resources to do so, employers will learn there is little risk to gaming the system and breaking the law.

Law abiding employers, however, will be forced to deal with the hassle and inconvenience of signing up for E-Verify and a biometric system. Then they'll be forced to watch and wait when they are blocked from putting lawful employees to work on the planned date due to system inaccuracies or other malfunctions. The inevitable result will be more, not fewer, employers deciding to pay cash wages to undocumented workers. Similarly, cash wage jobs will become attractive to workers who have seemingly intractable data errors. Instead of reducing the number of employed undocumented workers, this system will create a new subclass of employee – the lawful yet undocumented worker.

Additional failures will come when the worker is initially processed through the system. Crooked insiders will always exist and be willing to sell authentic documents with fraudulent information.[20] Undocumented immigrants will be able to contact these crooked insiders though the same criminals whom they hired to sneak them into the United States. Securing identification will simply be added to the cost of the border crossing.

Worse, since 2004, more than 260 million records containing the personal information of Americans have been wrongly disclosed.[21] Many individuals' personal information, including social security numbers, are already in the hands of thieves. There is nothing to prevent a criminal from obtaining fraudulent access to E-Verify (pretending to be a legitimate employer), verifying that a worker is not already registered in the system and sending an undocumented worker to get a valid biometric using someone else's information.

Additional problems inherent in any biometric will materialize both when an individual is enrolled, and at the worksite. For example, according to independent experts there are a number of problems that prevent proper collection and reading of fingerprints, including:

- Cold finger

[20] Center for Democracy and Technology, "Unlicensed Fraud." January 2004 (www.cdt.org/privacy/**2004**0200dmv.pdf).

- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint; and
- Manual activity that would mar or affect fingerprints (construction, gardening).[22]

When these failures occur it will be difficult and time consuming to re-verify the employee. Running the print through the system again may not be effective, especially if the print has been worn or marred. Returning to the biometric office for confirmation of the print is not likely to be a viable solution because it creates another potential for fraud; the person who goes to the biometric office may not be the person who is actually applying for the job. These are complex security problems without easy solutions.

There would also be mounting pressure to "fix" many of these problems with more databases filled with identifying information such as birth certificates or DNA in an attempt to identify individuals earlier and more completely. This would mean more cost, more bureaucracy and less privacy. From a practical point of view a biometric system is the worst of both worlds. It puts enormous burdens on those already obeying the law while leaving enough loopholes so that lawbreakers will slip through.

III. A Biometric National ID System Will Trammel Privacy and Civil Liberties

The creation of a biometric national ID would irreparably damage the fabric of American life. Our society is built on privacy, the assumption that as long as we obey the law, we are all free to go where we want and do what we want – embrace any type of political, social or economic behavior we choose. Historically, national ID systems have been a primary tool of social control. It is with good reason that the catchphrase "your papers please" is strongly associated with dictatorships and other repressive regimes. As Americans, we have the right to pursue our personal choices all without the government (or the private sector) looking over our shoulders monitoring our behavior. This degree of personal freedom is one of the keys to America's success as a nation. It allows us to be creative, enables us to pursue our entrepreneurial interests, and validates our democratic instincts to challenge any authority that may be unjust.

A biometric national ID system would turn those assumptions upside down. A person's ability to participate in a fundamental aspect of American life – the right to work – would become contingent upon government approval. Moreover, such a system will almost certainly be expanded. In the most recent attempt to create a national ID though a state driver's license system called Real ID, at the outset the law only controlled access to federal facilities and air travel. Congressional proposals quickly circulated to expand its use to such sweeping purposes as voting, obtaining Medicaid and other benefits, and traveling on interstate buses and trains.[23]

---

[22] International Biometrics Group, http://www.biometricgroup.com/reports/public/reports/biometric_failure.html

[23] See, e.g. H.R. 1645, the Security Through Regularized Immigration and a Vibrant Economy Act of 2007 (110th Congress).

Under a national ID system, every American would need a permission slip simply to take part in the civic and economic life of the country.

The danger of a national ID system is greatly exacerbated by the huge strides that information technology ("IT") has made in recent decades. There is an enormous and ever-increasing amount of data being collected about Americans today. Grocery stores, for example, use "loyalty cards" to keep detailed records of purchases, while Amazon keeps records of the books Americans read and airlines keep track of where they fly. Congress has acknowledged these practices and has held numerous hearings to discuss the issues of online privacy.[24] A biometric national ID system would add to these problems by helping to consolidate this data.

The sordid history of national ID systems combined with the possibilities of modern IT paint a chilling picture. These problems cannot be solved by regulation or by tinkering around with different types of biometrics. Instead, the entire unworkable system must be rejected so that it does not intolerably impinge on American's rights and freedoms.

VI. Conclusion: Congress Must Not Enact a Mandatory Employment Eligibility Pre-Screening System

The goal of E-Verify is to reduce the number of unauthorized workers in the United States. Unfortunately, its success rate is extremely low. According to the CIS's Westat report the inaccuracy rate for unauthorized workers is approximately 54 percent.[25] According to the government's own reports, **E-Verify is fulfilling its intended purpose less than half the time**. In addition, experience in Arizona shows that many employers are failing to comply in spite of it being a state mandate. Therefore, while E-Verify continues to burden employers, cost the government billions of taxpayer dollars, and deny Americans' their right to work—all the while potentially subjecting them to discrimination—it is not even adequately performing its core function.

The ACLU urges the Subcommittee to reject imposition of a mandatory electronic employment eligibility pre-screening system and the use of any biometric system. Each would cause great harm to employers across the country and to lawful workers and their families while doing little to dissuade undocumented workers. The likelihood for harm is great and the prospect for gain has so far proved illusory.

---

[24] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009); *The State of Online Consumer Privacy: Hearing before the S. Commerce, Science and Transportation Committee*, 112th Cong. (2011).

[25] 2009 Westat Report at 118.